UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA, :

v. : Indictment No. 15-cr-866 (WHP)

: **DECLARATION**

ROGER THOMAS CLARK, :

Defendant. :

----------x

I, JOSHUA L. MICHEL, declare under penalty of perjury, pursuant to 28 U.S.C. §1746, that the following is true and correct:

Background

1. I am employed by Roloff Digital Forensics, LLC a company that specializes in analyzing electronic evidence in criminal law proceedings.

2. Roloff Digital Forensics, LLC was retained by Jacob Mitchell and Stephanie Carvlin, attorneys for Roger Thomas Clark, to review the government's explanation of how law enforcement, specifically Federal Bureau of Investigations ("FBI") Special Agent Christopher Tarbell, claimed he found the Internet Protocol ("IP")[1] address for the Silk Road website.

3. In a Declaration by Agent Tarbell, provided to me by the defense (Exhibit C to Jacob Mitchell Declaration at ¶ 7), Agent Tarbell claimed that he

[1]An Internet Protocol address or IP address is a numerical address that is akin to a physical address for a home but is for a computer.

and another member of the FBI found the Silk Road server's IP address by a technique known as packet sniffing:[2]

4. Data sent through the Internet is broken into "packets" – or bits – that consist of header bits and payload bits. The header contains the source and destination IP addresses, and other information that is needed to get the data from Point A to Point B. The payload is the data to be transported.[3] For example, the contents of an email would be the payload. The IP address of the sending and receiving computers would be part of the header.

5. In his Declaration, Agent Tarbell detailed how he and his fellow agent found the Silk Road IP address:

> In or about early June 2013, another member of CY-2 and I closely examined the traffic data being sent from the Silk Road website when we entered responses to the prompts contained in the Silk Road login interface. This did not involve accessing any administrative area or "back door" of the site. We simply were interacting with the website's user login interface, which was fully accessible to the public, by typing in miscellaneous entries into the username, password, and CAPTCHA fields contained in the interface. When we did so, the website sent back data to the computer we were using – specifically, the Silk Road homepage, when we used valid login credentials for undercover accounts we had on the site, or an error message, when we used any username, password, or CAPTCHA entry that was invalid.
>
> Upon examining the individual packets of data being sent back from the website, we noticed that the headers of some of the packets reflected a certain IP address not associated with any known Tor

---

[2]Packet sniffing is the act of intercepting packets as they traverse the network and then viewing the packets and their contents. This is typically done with a computer program designed for this purpose such as Wireshark.

[3]Agent Tarbell affirmed that he and his fellow agent examined the individual packets of data sent back from the Silk Road website and "noticed" the headers of some packets reflected non-Tor IP addresses. He does not say what portions of the packets he examined.

> node as the source of the packets. This IP address (the "Subject IP Address") was the only non-Tor source IP address reflected in the traffic we examined. The Subject IP Address caught our attention because, if a hidden service is properly configured to work on Tor, the source IP address of traffic sent from the hidden service should appear as the IP address of a Tor node, as opposed to the true IP address of the hidden service, which Tor is designed to conceal. When I typed the Subject IP Address into an ordinary (non-Tor) web browser, a part of the Silk Road login screen (the CAPTCHA prompt) appeared. Based on my training and experience, this indicated that the Subject IP Address was the IP address of the SR Server, and that it was "leaking" from the SR Server because the computer code underlying the login interface was not properly configured at the time to work on Tor.[4]

6. I conducted an analysis of the Silk Road servers associated with IP addresses 193.107.86.49 (".49") and 62.75.246.20 (".20") to attempt to confirm or rebut Agent Tarbell's explanation.

My Credentials

7. I am a senior forensic examiner at Roloff Digital Forensics, LLC a private digital forensics firm with offices in Spokane Washington, Portland Oregon, and Copperopolis California. Roloff Digital Forensics provides digital forensics services and consultation on legal matters that pertain to electronic evidence.

8. My educational background includes the EnCase Certified Examiner (EnCE) certificate from Opentext, the Cellbrite Certified Operator (CCO) certificate, the Cellbrite Certified Physical Analysst (CCPA) certificate and the Cellbrite Certified Mobile Examiner (CCME) certificate. I studied computer science at Eastern Washington University.

---

[4]The footnotes in the paragraph designations are omitted from this excerpt of Agent Tarbell's Declaration. A complete version of the Declaration is Exhibit C to the Jacob B. Mitchell Declaration.

9. I have been working exclusively in the field of digital forensics since March of 2013. During this time I have conducted examinations on thousands of digital evidence items including: hard drives, flash drives, thumb drives, compact discs (CDs), digital versatile discs (DVDs), Blu-ray discs, magnetic tapes, tablet devices, cellular phones, subscriber identity modules (SIM) cards, personal digital assistants (PDAs), smart phones, feature phones, video surveillance systems, video game systems and data derived from service providers such as Internet Service Providers (ISPs), online "cloud" storage providers and cellular service providers. During my tenure within the digital forensics field I have completed over 500 cases that involved analysis of these various media types. I would estimate I have received over 1000 hours of training specific to digital forensics.

10. I have lectured on the topic of digital forensics and how it can be applied to the legal system. I have been recognized as an expert in digital and mobile forensics as well as digital photography in numerous United States District Courts, United States Military Courts and State Courts throughout the country.

11. The list of clients in these matters include the United States Navy, United States Marine Corps, United States Army, United States Air Force and the United States Coast Guard, Federal and State Public Defenders offices throughout the United States and private attorneys throughout the United States and in Europe. I have investigated digital evidence in allegations of sexual

assault, homicide, child exploitation, hacking, kidnapping, espionage and theft of trade secrets.

12. I have knowledge and experience in Linux, Nginx, Apache, MySQL, PHP and TOR software and operating systems.

Scope of My Review

13. In undertaking my analysis, I reviewed the following materials:[5]

a. 8 terabytes of data produced by the government on July 16, 2018, including the images of the .49 server and one image of the .20 server.

b. the indictment in *United States v. Ulbricht*, 14-cr-68 (KBF) (Exhibit A to Jacob Mitchell Declaration at ¶ 7).

c. the indictment in *United States v. Clark*, S2 15-cr-866 (WHP) (Exhibit B to Jacob Mitchell Declaration at ¶ 7).

d. the Declaration of Agent Christopher Tarbell Doc. 57 filed in connection with the *Ulbricht* prosecution in which the Agent provided an explanation for the steps he undertook to locate the IP address of the .49 computer; (Exhibit C to Jacob Mitchell Declaration at ¶ 7).

e. the Declaration Of Joshua J. Horowitz filed in *United States v. Ross Ulbricht*, 14-cr-68 (KBF), in support of Mr. Ulbricht's

[5]Before providing me with the material, Mr. Mitchell sent me a copy of the Protective Order in this case to me. I have read the Order and understand that I am bound by its terms.

motion to suppress evidence and the exhibits to the Declaration; (Exhibit D to Jacob Mitchell Declaration at ¶ 7).

f. the Government Response To The Declaration Of Joshua Horowitz; (Exhibit E to Jacob Mitchell Declaration at ¶ 7).

g. the October 7, 2014 Letter to Judge Forrest by Joshua L. Dratel.[6] (Exhibit F to Jacob Mitchell Declaration at ¶ 7).

h. An Index of the 8 Terabytes of data produced in discovery by the government. (Exhibit F to Jacob Mitchell Declaration at ¶ 7).

How the Silk Road Server Was Configured and How that Bears on Agent Tarbell's Explanation for How the Silk Road Server's IP Address was Discovered

14. Based on my review of the images of the servers with the IP addresses 193.107.86.49 and 62.75.246.20 and the other material detailed above, I was able to reach the conclusions that follow.

15. When the image of the .49 server was captured, Silk Road was being run on the Ubuntu operating system, version 12.04.2. Ubuntu is a Linux-based open-source operating system. The server utilized Nginx, a performance web server,[7] capable of handling high volumes of traffic.

16. The material provided to me by defense counsel shows that when the images of the servers were made, the Silk Road website was split between two different servers: a front-end server and a back-end server. The .20 IP address

[6] In addition, I also reviewed the contents of eight terabytes of discovery provided by the government to the defense on July 16, 2018. My conclusions are based on my analysis of the materials detailed above.

[7] A server is a host computer that sends data to and receives data from client computers and other servers.

server functioned as the front-end, and the .49 IP address was the back-end.

17. The access logs to the .20 and .49 servers show that the .20 server, which the government has stated was the IP address of one of the Silk Road servers, was constantly requesting information from the .49 server. This demonstrates that the .20 server functioned as the front-end server, and the .49 server functioned as the back-end server.

18. Agent Tarbell claims he obtained access to the Silk Road CAPTCHA prompt, by typing "the subject IP address into an ordinary non-Tor web browser[.]" (Tarbell Declaration, Exhibit C to Mitchell Declaration, at ¶7.)

19. The CAPTCHA prompt for the Silk Road website is contained on the back-end server – the .49 server.

20. Based on the server-configuration files provided in discovery, direct access to the back-end server (the CAPTCHA prompt) should not have been possible.

21. The back-end Silk Road web server –.49 – only permitted access through the front-end server - .20.

22. The back-end server hass two file folders that controlled access. On Silk Road the file folders were labeled "sites-available" and "sites-enabled."

23. To be activated, the "sites-enabled" folder had to have a link to a configuration file in the "sites-available" folder.

24. The sites-enabled folder contains two links only – one to the live-ssl and one to the phpmyadmin files.

25. The live-ssl configuration controlled access to the underlying market

data which is where the CAPTCHA is contained on the .49 server.

26. The following configuration lines from the live-ssl files is the code that controls access to the CAPTCHA:

```
allow 127.0.0.1;
allow 62.75.246.20;
deny all;
```

27. This code tells the web server (.49, the back end) to allow access from IP addresses 127.0.0.1 and 62.75.246.20 and *deny* access to all other IP addresses.

28. The IP address 127.0.0.1 is commonly referred to in computer networking as "localhost", meaning the machine itself. Thus, the line 127.0.0.1, enables the server to connect to itself.

29. In other words, the .49 back-end server was configured to refuse connections from all outside IP addresses with only two exceptions: the front-end server – the .20 server – and itself.

30. Based on this configuration it is implausible that Agent Tarbell accessed the portion of the .49 server containing the Silk Road, including the CAPTCHA, simply by entering the IP address of the server in his browser.

31. I've reviewed 19 lines of the Nginx access log for [.49 server], which I've been informed by defense counsel is the only documentation of Agent Tarbell's discovery of the Silk Road website's IP address in early June of 2013. The 19 lines of access logs do not show in any detail the steps which may have lead to the discovery of the Silk Road server IP address.

The Lack of Documentation of Agent Tarbell's Work

32. I have Certifications in industry standard tools, Cellbrite and Encase,

which are accepted widely in the forensic community as certifications that, when achieved, demonstrate competent understanding and mastery of digital forensic standards.

33. Based on my Cellbrite and EnCase training and experience, I am aware of the standards and best practices used by forensic computer examiners and are commonly known and understood among my colleagues.

34. I received training on best practices in order to achieve each certification above. Continuing training is required regularly to maintain those certifications, and these practices are frequently discussed and commonly understood to be used at all times.

35. The touchstones of digital forensic investigation are: identification, collection, acquisition and preservation of digital information and then testing, analysis and reporting on the investigation of that information.

36. The best practices and standards for analysis and reporting require the examiner to document actions and procedures undertaken during testing, examination and analysis and then if possible, verify those findings and if need be conduct further testing and analysis, this process can be iterated as long as necessary to reach a verifiable and repeatable outcome.

37. Since Agent Tarbell provided no records documenting his procedures processes or methodologies that led to the discovery, it is apparent he did not adhere to those standards and best practices.

38. As discussed *infra* at ¶3, the process that agent Tarbell described using to locate the Silk Road website is packet sniffing. Packet sniffing programs

can easily, automatically save detailed information about each packet that is transmitted or received. In fact, this is common due to the volume of information that is being generated. There is simply too much data being received to conduct any meaningful analysis without saving the material. In 2013, the most common tool utilized for such activities was Wireshark, whose default configuration was set to save logged information. Before exiting the program, a user would be prompted as follows: "Do you want to save the captured packets before quitting? Your captured packets will be lost if you don't save them."

Dated: October 29, 2019

Spokane, Washington

Joshua Michel, EnCe, CCO, CCPA, CCME